System Hardening

Defense in Depth—at home and on the road

System Hardening

- Wi-Fi security
  - At home
  - Away from home
- Windows system hardening
- Mac OS X system hardening

KU THE UNIVERSITY OF KANSAS

Wi-Fi security

- Question 1: Do I need wi-fi?
  - Don't own any wireless devices? Don't buy a wireless router!
  - A regular, wired-only router is cheaper and offers one less attack vector

Most wireless routers also offer the option to disable the wireless radio. If you bought a wireless router but aren't using the wireless functionality, turn off the radio!

Wi-Fi security

- Question 2: What kind of wireless router should I buy?
  - What are your needs?
    - Basic connectivity?
    - Blazing speeds?
    - Good security?
    - Cost?
    - Bleeding-edge technology?

KU THE UNIVERSITY OF KANSAS

The upper speed limit of an 802.11g network is 54Mbps (megabits per second) but some routers come with channel bonding features that allow you to “double” that speed—they will advertise themselves as being 108Mbps 802.11g networks. These routers require that you buy specific wireless adapters that allow you to take advantage of that features. Without the fancy adapters, you’re still just using plain old 54Mbps 802.11g. Netgear calls it “Super-G,” Linksys calls it “SpeedBooster” or “SRX.” Other companies may have different names for it—just keep an eye out for claims of “108 Mbps.” Unless you plan to buy the compatible adapter, it’s generally a waste of your cash.

What about 802.11n?

•Also called “pre-N,” “draft N,” and “MIMO” (Multiple Input Multiple Output)

•Will be officially adopted March 2009, advertised starting December 2009 (vendors are getting the jump on the standard)

•You must have an 802.11n adapter in your computer

•802.11n can “dummy down” for 802.11a/b/g devices

- •This **WILL** affect your network’s performance in a negative way

•802.11n is a draft standard, which means it may change between now and when it is officially adopted

- •While this is a risk, it appears to be an unlikely one

Wi-Fi security

- Security is *paramount* when it comes to wireless router selection
  - WEP is essentially worthless—don't rely on it to encrypt your data
  - WPA-PSK can be cracked easily if the Pre-Shared Key is weak
  - Look for devices that use WPA2 (also called 802.11i or AES) security

KU THE UNIVERSITY OF KANSAS

WEP (Wired Equivalent Privacy: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) used to be considered "better than nothing." It could be cracked, but it took a long time and most people felt that all but the most determined attackers wouldn't attempt it. Recent developments in the security research world have shown that WEP can be cracked in less than one minute—giving attackers easy access to your network and your data.(http://www.theregister.co.uk/2007/04/04/wireless_code_cracking/)

WPA (Wi-Fi Protected Access: http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) is a far superior method of securing wireless communications on your home network. It can be cracked, however, if you are using WPA-PSK (or WPA Personal) and the Pre-Shared Key is weak. Look for devices that use WPA2 (also called 802.11i) security.

Older wireless adapters may have trouble with the WPA2-AES encryptions standard—you may have to downgrade to WPA-TKIP, but don't go any further than that.

Wireless Router Hardening

- Consider placing your router away from exterior walls and windows
  - In an apartment complex, preventing signal leakage can be difficult to impossible
  - Farther away from roads/sidewalks may help deter wardriving

KU THE UNIVERSITY OF KANSAS

This can be tough to do based on where you live, where the cable/phone jacks are in your house, etc.

Materials like concrete (especially reinforced) kill signal strength. If your wireless router is in the basement, don't expect good (or any) signal in the second floor of your house.

Wireless Router Hardening

- Patch, patch, patch!
  - Only upgrade firmware from a wired connection
  - Back up your current configuration first
- Use the strongest encryption available
  - Use a strong pre-shared key

KU THE UNIVERSITY OF KANSAS

So I bought my new wireless router/I already own one. What can I do to make it safer?

Random password generator:

http://www.pctools.com/guides/password/

Use the longest, most random pre-shared key possible. Include upper and lower case letters, numbers, and special characters. Save it to a USB key or print it out—then store it in a safe place.

Wireless Router Hardening

- Change the admin password on the router
- Change the default SSID
  - This the name of your wireless network
- Disable SSID broadcast *(optional)*
  - Some devices may fail to connect if you do this
- Enable MAC address filtering
  - This has nothing to do with Macintoshes ☺
  - MAC addresses can be spoofed

KU THE UNIVERSITY OF KANSAS

Admin password: Proof of concept exploits exist that can allow an attacker to take control of your router by convincing you to visit a maliciously crafted web page. Use a strong password here!

These are good tips but should not be relied upon exclusively for security. They only slow a determined attacker down—they will not stop him/her.

Disabling the SSID broadcast is trivially easy to defeat. If it breaks any of your devices' ability to connect to the router, turn SSID broadcast back on—it doesn't help security so much that it's worth the loss in functionality.

SSID: Service Set Identifier

Wireless Router Hardening

- Limit the number of connections allowed
  - Only have four devices? Configure DHCP to only distribute four IP addresses
  - Change the default IP address of your wireless router
- Disable Remote Management
- Disable “respond to ICMP Ping”

KU THE UNIVERSITY OF KANSAS

Wireless Router Hardening

- Disable the DMZ (Demilitarized Zone)
  - Any computer in the DMZ is completely open to the internet (and open to attack)
- Disable UPnP
  - Some services (like Microsoft's XBox Live! or MSN Messenger file transfers) need UPnP

KU THE UNIVERSITY OF KANSAS

For more on UPnP (Universal Plug and Play)
http://www.grc.com/unpnp/unpnp.htm

Wireless Router Hardening

- Change the default IP address of the router
  - This will usually be something like 192.168.0.1 or 10.0.0.1
  - This may be required (DSL modems like to use the 192.168 range) but it may also break things
- Enable the firewall
  - If your router has a firewall built in, use it!
  - This may block some ports for gaming or other applications

KU THE UNIVERSITY OF KANSAS

Many AT&T DSL modems require use of the 192.168.*.* (where the * represents a wild card) IP range and cannot be reconfigured to use anything else. (I have configured routers on both Sunflower and Cox cable systems and not run into this issue.) For this reason, many new routers have switched to the 10.0.*.* range. If your router is handing out 10.0.*.* IP addresses, this may conflict with the KU Anywhere VPN service. If you're having problems, try changing your router's IP address to 192.167.0.1 or perhaps 10.1.0.1. See your router's user manual or call your manufacturer's support line for assistance with this.

Many Netgear routers use the www.routerlogin.com address to access the administrative interface for the router. Changing the router's IP address may make the www.routerlogin.com address no longer work. No worries—just make sure you write down your router's IP address and type THAT number into your browser whenever you need to change your router's settings.

Most programs that need inbound access (open ports on the firewall) will tell you which ports (or range of ports) they require. Rather than disabling the firewall when a program doesn't work, find out which ports it needs and open only those ports up!

Wireless Router Hardening

- Consider switching to OpenDNS
  - Instead of obtaining DNS settings from your ISP, manually configure the router to use OpenDNS servers
  - Helps filter out malicious websites, can also filter other types of “blue” content
    - Content filtering is user configurable

KU THE UNIVERSITY OF KANSAS

Nameservers are 208.67.222.222 and 208.67.220.220

http://www.opendns.com/how/dns/turning-names-into-numbers

Some people have privacy concerns with OpenDNS. Depending on how sensitive you are to these issues, you will want to review their privacy policy prior to using their service.

Advanced Wireless Router Concepts

- Feeling a little geeky? Hack your wireless router
- Linksys WRT54GL platform is *fantastic* for this
  - Other routers are hackable too—check your make/model
- YOU MAY “BRICK” YOUR ROUTER.

KU THE UNIVERSITY OF KANSAS

More router hacking resources:

http://www.wrt54ghacks.com/

Linksys WRT5 Ultimate Hacking by Paul Asadoorian and Larry Pesce

Some open source firmwares:

OpenWRT (are you comfortable at the command line?)

DD-wrt (more user friendly)

Tomato

LOTS of others—kind of depends on your goals

Securing your network…

- Get rid of old wireless hardware
  - Older wireless cards may not support new encryption standards
  - Buy a new router if yours only supports WEP

KU THE UNIVERSITY OF KANSAS

Some routers can be flashed with a new firmware that allows WPA encryption—check for that before you throw your old router out!

Personal Computer Security

- Develop some new good habits
- Remember, cybersecurity breaks **can** and **will** happen to you
- An ounce of prevention is worth a pound of cure!

Personal Computer Security

- No matter your platform, you should…
  - Have a separate account for each user on the system
  - Protect ALL accounts with a password
  - Conduct day-to-day computer usage as a “non-privileged” user
  - Use an inactivity time-out that locks the screen
  - Use a firewall
  - Perform regular backups
  - Use antivirus software (yes, Mac users, you too!)

KU THE UNIVERSITY OF KANSAS

Computer Accounts

- For our purposes, there are two types of accounts on a system:
  - Administrator (or root)
  - User (or non-privileged user)
- Administrator accounts have unlimited power
  - With great power comes great responsibility *(nerd alert! ☺)*
  - Administrator accounts are needed to install new software, configure network settings, install printers, etc.
  - Malicious websites and programs take advantage of that power to compromise your system

KU THE UNIVERSITY OF KANSAS

If you're using your computer as an administrator, you're more vulnerable…than you would be if you used your computer as an unprivileged user. Unprivileged users typically can't install software on the computer or if they can, the software should only run in that particular user's security context, meaning only when that user is logged in and only with the capabilities of that user. In other words, if you run as a regular user, you won't be able to trash your entire computer as easily.

Computer Accounts

- "User" or "non-privileged" accounts
  - Generally can't install software (any programs installed will run at that user's privilege level)
  - Can't make configuration changes to firewall, AV, and other critical system components

KU THE UNIVERSITY OF KANSAS

Running as a non-privileged user

- Good news:
  - Much, much less vulnerable to “drive by downloads” and other malware
  - Much less likely to accidentally modify settings to critical system components
  - In many cases, any malware infecting the system will be forced to run at a non-privileged level as well, greatly limiting the damage it can do

KU THE UNIVERSITY OF KANSAS

Running as a non-privileged user

- The “bad” news:
  - If you want to make configuration changes or install software, you’ll have to log out and log back in as an administrator
    - In Windows, the “Run As…” command can help you get around this
  - Some programs misbehave when asked to run at a non-privileged user level
    - some developer tools
    - some games

Computer Security: The Basics

- Many security problems can be alleviated just by keeping your software up to date!
  - Enable Automatic Updates (Win) or System Update (Mac) to download and install automatically
  - Allow add-on programs like Adobe Reader and QuickTime to check for updates automatically

KU THE UNIVERSITY OF KANSAS

Computer Security: The Basics

- Uninstall software you no longer use
  - Forgotten, unpatched software may make your machine more vulnerable
- Look gift horses in the mouth
  - Just because that blinking ad banner says to download that free software doesn't make it a good idea!

KU THE UNIVERSITY OF KANSAS

Computer Security: Firewalls

- Both Windows and Macintosh computers come with firewalls
  - Windows XP Service Pack 2 enables the built-in firewall by default
  - Mac OS X *does not* enable its firewall by default

KU THE UNIVERSITY OF KANSAS

For more on firewalls: http://www.besekure.ku.edu/~privacy/cgi-bin/mydrupal/?q=node/25

Computer Security: Firewalls

- To enable the Windows XP Internet Connection Firewall (ICF):
  - Click Start→Control Panel and select Security Center
  - Under "Manage security settings for:" click Windows Firewall. Make sure that the radio button next to "On" is selected.
  - If you open this panel and find that your firewall options are “greyed out,” there is a good chance your computer is infected with malware.

KU THE UNIVERSITY OF KANSAS

Computer Security: Firewalls

- The Windows XP firewall does not do any outbound filtering by default.
  - Consider a 3rd party firewall
  - Many good free options, even more good paid options
  - Free: ~~Comodo Firewall Pro,~~ ZoneAlarm
  - Paid: Kerio, ZoneAlarm, simple home router/firewalls (network-based)

KU THE UNIVERSITY OF KANSAS

I hesitate to recommend the Comodo free firewall product. I used to use it myself until it began to be bundled with the Ask toolbar, a toolbar many anti-spyware programs identify as spyware.

Computer Security: Firewalls

- Windows Vista firewall
- Looks and feels just like XP firewall
  - Unlike XP, does inbound *and* outbound filtering
- Access via Control Panel→Security Center→Windows Firewall
- Network based firewall is still a good addition!

KU THE UNIVERSITY OF KANSAS

Advanced users can modify firewall settings at Control Panel→Administrative Tools→Windows Firewall with Advanced Security

Heavier-duty technical analysis of the Windows Vista Firewall can be found at http://www.sans.org/reading_room/whitepapers/firewalls/1861.php

From the whitepaper: “The Vista firewall provides simple and effective protection and clearly is not intended to be a single security solution. It’s cost effective as being distributed as part of the OS and offers a sense of purity in what it does. Combined with other facilities such as anti-virus and patch management, it can still be thought of as that 3rd piece of an overall PC protection posture.”

Computer Security: Antivirus

- Antivirus ≠ panacea!
- Antivirus software is a piece of the puzzle—just one layer of Defense in Depth
- Antivirus software is a corrective measure at best, a detective measure most of the time, and totally ineffectual in some cases
- Even though it can't fix every problem, *no computer should be without it.*

KU THE UNIVERSITY OF KANSAS

Computer Security: Antivirus

- Allowing your antivirus software to become outdated is as bad as not having any at all.
- If you have an always-on internet connection, set your software to check for updates at least every 30 minutes (Sophos is set this way by default)
  - Dial-up users should check for updates at least once a day
- Never, ever attempt to run more than one antivirus software package at once!

KU THE UNIVERSITY OF KANSAS

Computer Security: Antivirus

- Sophos is free to KU students, faculty, and staff
  - You have other options, some free, some not
  - If you need technical assistance with Sophos, you can call the IT CSC at 4-8080

KU THE UNIVERSITY OF KANSAS

Computer Security: Anti-spyware

- There are several excellent free anti-spyware tools available
- Any package with “active protection” *may* conflict with your antivirus software
  - Many AV packages now contain anti-spyware pieces as well (check with your vendor)
- “Passive protection” *shouldn’t* cause a problem
  - These products “play nicely” with Sophos, but check with your vendor if you aren’t using Sophos!

KU THE UNIVERSITY OF KANSAS

Computer Security: Anti-spyware

- Removal and prevention:
  - Spybot Search & Destroy
    - check for signature updates weekly, don't forget to immunize!
  - Microsoft Windows Defender
- Removal only:
  - Ad-Aware 2007
    - paid version offers active protection
- Prevention only:
  - Spyware Blaster
    - check for updates weekly
    - paid version offers automatic updates

KU THE UNIVERSITY OF KANSAS

MacScan: Not free, but one of the few Mac-based malware options.
http://macscan.securemac.com/

Computer Security: Other utilities

- CCleaner
  - Removes temp files, cache, cookies, stray registry keys
    - saves HD space, may remove bits of malware
- Trend Micro Housecall
  - http://housecall.trendmicro.com
  - Free web-based virus and malware scan/removal tool
    - Won't conflict with your antivirus software

Computer Security: Surf Safer

- Get away from using Internet Explorer as your primary browser
  - Switch to Firefox for day-to-day browsing (you too, Mac users)
  - Use add-ons to make surfing even safer
  - Keep your helper apps (Acrobat, QuickTime, etc) updated

KU THE UNIVERSITY OF KANSAS

Safari contains no anti-phishing measures. Internet Explorer for Mac was EOLed (end-of-life'd) by Microsoft several years ago and should not be used. Google Chrome is too new to be relied upon exclusively.

Computer Security: Surf Safer

- Hardening Firefox
  - Tools→Options (Firefox→Preferences on Mac OS X)
  - Warn about add-ons, warn about forgeries should both be checked
  - *Uncheck* “remember passwords for sites”

KU THE UNIVERSITY OF KANSAS

More Firefox hardening…

- addons.mozilla.com has lots of add-ons for Firefox:
  - NoScript (blocks scripted content from running)
  - Adblock Plus (blocks ads and possible malicious page elements)
  - Filterset.G updater (downloads preconfigured filterset for Adblock Plus)
  - Plugins work in Firefox for the Mac too!
- McAfee SiteAdvisor www.siteadvisor.com
  - can help prevent you from clicking on malicious websites by warning you about their content

KU THE UNIVERSITY OF KANSAS

Internet Explorer Hardening

- IE 7 has *some* built-in anti-phishing features, IE 6 does not
  - McAfee Siteadvisor is also available for IE!
  - Google Toolbar has some nice anti-phishing features as well
  - Only use Internet Explorer when a site doesn't function properly in Firefox

KU THE UNIVERSITY OF KANSAS

Computer Security: Mac OS X

- Despite what you hear in the ads, Macs can:
  - Get hacked
  - Get malware
  - Get viruses

KU THE UNIVERSITY OF KANSAS

Computer Security: Mac OS X

- Mac OS X is a pretty GUI shell on a powerful UNIX OS
  - Playing with things you don't fully understand (or know how to harden) makes your computer *extremely vulnerable* to hackers
  - The power of Mac OS X makes it a very flexible platform for hackers, too!

KU THE UNIVERSITY OF KANSAS

Computer Security: Mac OS X

- Remember all that stuff we said about Windows? If you run Windows in Paralells, VMWare, or via BootCamp, it applies to you too!
- While Mac OS X isn't vulnerable to Windows viruses, worms, and malware, you can retransmit these items via e-mail or infected files

KU THE UNIVERSITY OF KANSAS

Computer Security: Mac OS X

- Many of the “best practices” we’ve already discussed apply to Mac OS X
  - “user” vs. “admin” accounts
  - use antivirus
  - use a firewall
  - beware of malware

Computer Security: Mac OS X

- To enable the built-in firewall:
  - Go to the blue Apple menu and select “System Preferences
  - Click Sharing pane, then Firewall tab
  - Check to see if the firewall is already on. If not, click “Start”
  - Make sure everything under “Allow” is *unchecked.*
  - Click the Advanced button.
  - Select Block UDP Traffic, Enable Firewall Logging, and Enable Stealth Mode.

KU THE UNIVERSITY OF KANSAS

Computer Security: Mac OS X

- Filevault
  - Encrypts your Home directory (*not* the entire hard drive)
  - Make sure you store the master password in a safe place—if it is lost, data cannot be recovered

KU THE UNIVERSITY OF KANSAS

Computer Security: Mac OS X

- Other security items from the Security Preference Pane:
  - Require password to wake from screen saver *(recommended)*
  - Disable automatic logins *(recommended)*
  - Log out after X minutes of inactivity
  - Use secure virtual memory
    - Depending on the security requirements of the data you handle, this may be desirable
  - Disable remote control infrared receiver
    - Again, it depends on your situation

KU THE UNIVERSITY OF KANSAS

Computer Security: Mac OS X

- Enabling services you don't know how to harden is a very, very bad idea!
- Turning on remote login or FTP virtually guarantees you'll get hacked
  - If you need a web host, use people.ku.edu or pay for hosting—turning on Personal Web Sharing introduces vulnerabilities as well

KU THE UNIVERSITY OF KANSAS

Corsaire white paper on OS X 10.5 hardening: http://research.corsaire.com/whitepapers/080818-securing-mac-os-x-leopard.pdf

On the Road: WiFi security

- Attackers may set up fake WiFi access points
  - Named things like “Free WiFi” or an SSID similar to the name of the place you’re sitting
  - Once you connect to these malicious hotspots, the attackers can set up “Man in the Middle” attacks, intercept your traffic, and steal your information

KU THE UNIVERSITY OF KANSAS

On the Road: WiFi security

- Only connect to trusted WiFi providers
  - How much do you *really* trust them?
- Use a VPN connection if you need to handle sensitive data
  - Never transmit or handle confidential information on an untrusted (or semi-trusted) without one!

KU THE UNIVERSITY OF KANSAS

On the Road: WiFi security

- Using your laptop but not connecting to a network? Disable the wireless radio!
  - Exploits exist for some Broadcom chipsets that do not require you to be connected to a network
  - This goes double for Bluetooth radios

KU THE UNIVERSITY OF KANSAS

On the Road: Laptop Security

- Taking a computer with you introduces additional security issues!
  - Higher risk of theft
  - Connecting to untrusted networks
  - Protecting data in case of theft

KU THE UNIVERSITY OF KANSAS

On the Road: Laptop Security

- Every account on your laptop should have a strong password!
- Use encryption, especially if you carry sensitive data with you
- Never leave your laptop unattended
  - Airports, libraries, coffee shops are all prime hunting grounds for laptop thieves
  - Conceal it in the car!

KU THE UNIVERSITY OF KANSAS

One free option for encryption is a utility called TrueCrypt. (www.truecrypt.org) You can use it to encrypt an entire drive or parts of it—it also works on USB keys.

While not free, PGP Whole Disk Encryption is a popular solution. www.pgp.com/products/wholediskencryption/

Security Testing @ Home

- ShieldsUP!
  - www.grc.com
  - Scans your computer for open ports, can help you identify problems (Windows and Mac OS X)
- LeakTest
  - www.grc.com
  - Tests your computer's firewall (Windows only)
- Microsoft Baseline Security Analyzer
  - www.microsoft.com/technet/security/tools/mbsahome.mspx
  - Windows only

KU THE UNIVERSITY OF KANSAS

Security Resources

- US-CERT Mailing Lists
  - www.us-cert.gov/cas/signup.html
- SANS Newsletters
  - www.sans.org/newsletters/
- SANS Internet Storm Center
  - isc.sans.org
- Microsoft Security At Home blog
  - www.microsoft.com/protect/default.mspx
- Apple Security Announce
  - lists.apple.com/mailman/listinfo/security-announce
- SecureMac.com
  - www.securemac.com

KU THE UNIVERSITY OF KANSAS

Questions?

Help us improve!

- Fill out an evaluation for this course at:
  - http://www2.ku.edu/~workshops/
  - Click “Evaluation”
  - Find “Basic System Hardening” (you may have to adjust the date range)

Contact

Julie C. Fugett, CISSP, CCE
Information Security Analyst
IT Security Office
(785)864-9003
jcf@ku.edu
www.security.ku.edu
www.besekure.ku.edu

KU THE UNIVERSITY OF KANSAS